Home Health Hub: A Secure and Interoperable Solution for Remote Patient Monitoring (RPM)

HIDS 505 Final Project Paper

Joelle Fitzgerald, Junaid Imam, Adam Li, Adi Patwardhan

Abstract

This paper addresses the growing challenge of managing chronic diseases and multimorbidity in the face of a projected 99.5% increase in chronic disease cases by 2050. With the rise of telehealth technology and accessibility, Remote Patient Monitoring (RPM) and telehealth services are emerging as effective methods of managing ongoing patient care. The paper examines the benefits and challenges of integrating RPM services, such as wearable devices and home monitoring devices, into routine healthcare, including the need for secure and seamless storage and communication of sensitive patient data. To address this need, the paper proposes a standardized method of cloud storage and interface for RPM services to ensure the safe and effective transmission of personal health information (PHI) between patients and their respective care teams. Our research recommends using a RPM vendor which is on the Redox network to ensure high levels of security, efficient, and in-depth EHR integration with specific stakeholder needs and industry objectives in mind. By integrating RPM services into routine healthcare, providers can offer patients the benefits of real-time patient monitoring, automated delivery of medicines, remote assistance via telemedicine, non-invasive medical procedures, reduced costs and re-admissions, and increased patient engagement and adherence to treatment plans.

Problem Statement & Overall Concept

Chronic disease is projected to increase by 99.5% from 71.5 million patients in 2020 to 142.6 million patients by 2050. At the same time, those with multimorbidity are projected to increase 91.16% from 7.8 million in 2020 to 14.9 million in 2050. The surge of telehealth technology and accessibility sparked by the COVID-19 pandemic has paved the way for remote patient monitoring (RPM) and telehealth services to rise in popularity as an effective and efficient method of managing ongoing patient care. The benefits of suitable prevention and adequate monitoring of chronic diseases by using emerging technological services such as wearable and at-home monitoring devices to collect health data in real-time, can increase the detection rates of health risks and raise the quality of life for elderly patients and those diagnosed with chronic conditions.

In 2020, 23.4 million American patients reported using RPM services including wearable devices, home monitoring devices, and other medical devices. Real-time patient monitoring, automated delivery of medicines, remote assistance via telemedicine, non-invasive medical

procedures, reduced costs and re-admissions, and increased patient engagement and adherence to treatment plans are all possible benefits of integrating RPM services into routine healthcare. However, Internet of Medical Things (IoMT) devices are constantly collecting sensitive and personal patient data, which poses the challenge of maintaining a secure and seamless system of storage and communication between RPM medical devices and the Electronic Health Record (EHR). As such, these devices provide a repository of data for hackers if proper security measures are not implemented. At least 82% of healthcare organizations have experienced a breach in their IoT devices. Therefore, care must be taken so that patient data doesn't fall into unauthorized hands. Our proposed project addresses the need for a standardized method of cloud storage and interface for RPM services in order to provide safe and effective transmission of personal health information (PHI) between patients and their respective care teams for prompt action and precise care management.

Solution to Meet Stakeholder Needs

The proposed technology will consist of two components: a home-based IoT device and a secure cloud-based interface. The IoT device will be designed to collect a patient's health data from various sources, including wearable devices and home monitoring devices - commonly prescribed by clinicians to track patient health status in order to inform patient care. The device will be equipped with advanced security features to ensure that the patient's health data is protected at all times and will serve as the central hub for the patient's health data. The interface will allow patients to easily upload their health data to the IoT device, monitor their health data, and share their data with their healthcare provider. The interface will also be integrated with the patient's EHR in correspondence to legal and ethical standards, allowing for seamless and secure transfer of health data - a mutually beneficial concept for all stakeholder interests. The proposed technology will have several benefits for patients and caregivers, healthcare providers, and healthcare organizations. For patients, the technology will provide a convenient and secure way to manage their health data, enabling them to take a more active role in their healthcare. Knowing loved ones are cared for, caregivers may experience less stress and anxiety, and more freedom to focus on work, family, and personal time. For healthcare providers, the technology will provide access to real-time health data, enabling them to provide more personalized and effective care. And, for healthcare organizations, the technology will provide a cost-effective way to manage and share health data, improving efficiency and reducing the risk of data breaches.

Furthermore, our solution is aligned with current industry goals of lowering healthcare costs and focusing on improving health outcomes for patients and populations. Following the Institute for Healthcare Improvement's (IHI) Triple Aim initiative for optimizing the health system performance through Value Based Care, integrated and interoperable RPM systems provide healthcare systems with the ability to streamline care using longitudinal and real-time

healthcare data to guide clinical practice. Gathering and joining continuous patient monitoring data with EHR systems improves all stakeholder experiences as health status surveillance reduces patient risk factors for disease, supplies physicians with ample data to make precise and prompt care decisions, thus lessening total healthcare costs and administrative burden to meet core measures. In addition, this interoperable and safe solution for managing the ongoing care of patients supports the Learning Healthcare System model by informing new methods, therapies, and guidelines for patient care incorporating the flow of generating new knowledge and data points which are embedded in daily practice (EHRs) to improve individual and population health.

Meaningful Use Objectives

Our solution corresponds with Meaningful Use requirements. Meaningful use defines the minimum United States government standards for EHRs to improve the collaboration between clinical and public healthcare, move towards patient-centric preventative care, and support the continued development of robust, standardized data exchanges. This outlines how clinical patient data should be exchanged between healthcare providers, providers and insurers, and providers and patients. Our interface solution will improve privacy and security for PHI while simultaneously improving patient engagement, care quality, and reducing health disparities. It also enables greater care coordination allowing remote patient data to be securely uploaded to EHRs in real-time. Providers have access to granular longitudinal data which allows them to track quality and cost improvement measures over time. This can help monitor the effectiveness of these efforts.

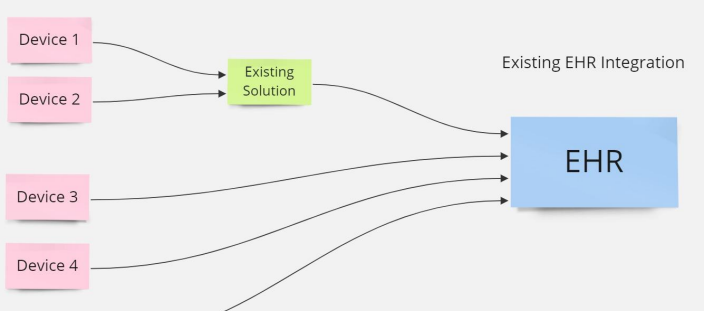
The Meaningful Use program was created to encourage healthcare providers to adopt electronic health records (EHRs) in hopes of improving patient care and safety, as well as the efficiency of healthcare delivery. RPM technology can help achieve these goals by enhancing patient engagement enabling patients to actively participate in their own care by providing them with real-time access to their health data. The Meaningful Use program includes several objectives related to patient engagement, patient safety, and care coordination. RPM technology can aid providers to meet these objectives by providing patients with access to their health data, enabling providers with resources to coordinate better care, and improving patient safety by reducing the risk of adverse events and progression of disease. RPM engages patients in the care process, thus improving their understanding of their health conditions and encouraging them to take a more active role in managing their health. By providing patients with the tools and information they need to manage their own health, RPM technology may also help reduce the overall burden on the healthcare system. Additionally, RPM integration is aligned with Meaningful Use's main goal of improving patient outcomes by helping providers identify potential health issues before they become acute, enabling earlier intervention and potentially better patient outcomes. By tracking patient data over time, providers can also gain a better

understanding of how patients respond to treatment, and adjust treatment plans as necessary. All of the benefits discussed above potentially reduce healthcare costs by enabling earlier intervention and identifying potential health risks, and therefore, preventing unnecessary hospitalizations and emergency department visits. Overall, RPM technology supports Meaningful Use incentives and objectives by improving patient engagement, patient outcomes, and care coordination, while also reducing healthcare costs.

Technical Infrastructure Requirements: Integration, & Interoperability

Factors for identifying and acquiring a new system that addresses safe and secure health data monitoring and sharing amongst home health devices and an EHR include: compatibility, connectivity, security, power source, scalability, data management and storage, cost, reliability and performance of the device, user interface, and technical maintenance. Compatibility of any device ensures that the device is harmonious with the existing systems and platforms that it needs to integrate with while also having strong security features to protect against potential cyber attacks and data breaches when dealing with protected health information. Interoperability while maintaining high performance and the ability to be scalable to changes and new features is also important for supporting stakeholder needs overtime. All of these selection criteria are important to note when formulating a working solution for interoperable home health monitoring devices.

Generally, the main components of the proposed solution requirements can be broken down into 3 categories: physical device interoperability, EHR integration, and cloud storage. Since the data is being pulled from medical devices, either raw or processed, it needs to be compatible with medical data standards, including but not limited to: LOINC, RxNorm, ICD, and CPT. While data standards play a big part in the compatibility checking, data is also generally accepted if some data is not in these formats, but such implementations will result in potentially reduced meaningful uses. To ensure the data collected from RPM devices can be integrated into an EHR system, some data quality checking and mapping is required. HL7/FHIR/OMOP will be the primary focus for this purpose. Writing continuous patient monitoring data into the EHR is not the end of the journey. For many purposes, including future data modification and examination, patient health data needs to be stored on the cloud for a varying length of time depending on the type and size of the data as well as stakeholder needs. Therefore, it is necessary to partner with HIPAA-compliant cloud providers with enhanced security features, such as AWS, GCP, and Microsoft Azure to ensure all patient health information remains safe and is only transferable to the appropriate parties in the right format at the right time (see Figure 1 & 2 below).



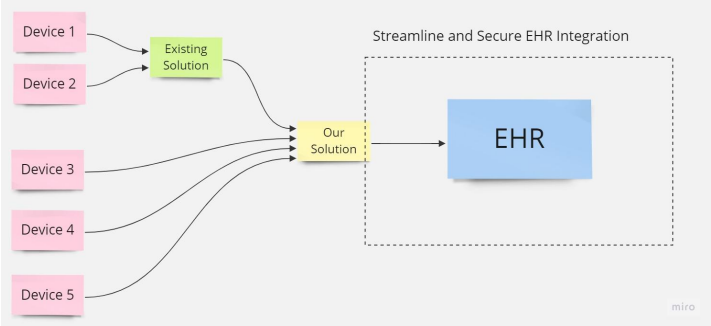


Figure 1 & 2: Sample current and proposed solution workflow

Standards, Security, & Challenges,

With many older medical devices still in use, the lack of wireless communication capability of these devices poses challenges for integration with an interface engine, thus limiting interoperability and data transmission. Due to the sensitive nature of health data being transmitted to and from these devices, security is the top concern for many healthcare providers as well as patients. The majority of healthcare organizations have experienced at least one breach in their IoMT devices, which raises safety risk questions about any new products and software targeting medical usage. To address this concern, a standardized security package is required to ensure stronger control while maintaining interoperability of both the physical devices and software. This standardization includes implementing a firewall on physical and digital layers, access control, data quality monitoring, breach alerts, higher end-to-end encryption level, device certification and audition, and routine maintenance. Other challenges that need to be addressed include abiding by legal data ownership and/or rights and terms of use of PHI according to HIPAA standards.

To ensure our proposed solution is secure, we developed our security measures broken down into four areas: on-device, data transmission, cloud, and administrative. We have minimum hardware and software requirements for our manufacturer and service provider partners to implement on their devices. For all devices that can connect directly to the internet, WPA 2 (Wi-Fi Protected Access Version 2), a Wi-Fi access control standard developed in the early 2000s

and now superseded by WPA 3, should be used when WPA 3 implementation is not available. The exact requirement applies to those requiring a hub to mediate the connection, and Bluetooth 4.0 is recommended to connect individual devices. When suitable, two-factor authentication is mandated, using a phone number, a security key, or any other second method for authentication should be used.

During the data transmission, it is required that all data is encrypted and sent over a secure network. Routing data through our dedicated VPN (Virtual Private Network) is optional but encouraged for additional security. To further enhance connection security while maintaining compatibility, asymmetric encryption is used for end-to-end encryption, where different keys are used when encrypting and decrypting data packets. Minimally, SSL (Secure Socket Layer) certificate is required when sending data over the HTTPS protocol.

Since we use cloud technologies to process, store, and transfer data, we propose a list of cloud security requirements. The firewall serves as the forefront layer of protection; thus, all ports are carefully set to disable or enable status, and any changes will require a security team meeting for review. Additionally, periodic port scanning needs to be implemented to catch any potential risks. Similar to the port settings, all traffic rules are semi-permanent once in effect unless the meeting calls for a modification. While data is on the cloud, all services should be isolated from each other and containerized when possible. The core idea is that each service is not affected when one or more are suspended after being flagged for problems and reviews. On top of the firewall intrusion detection, data processing services need to be able to intercept and flag suspicious packets and suspend the workflow before setting off the security alert. To ensure the data storage is secure, we aim to distribute our databases and have a hot backup when a threshold of operation amount is met, plus a complete backup periodically. To lower the likelihood of service downtime, the cloud infrastructure has to be elastic, meaning that it will automatically scale to fit the operational requirements. When the system is inevitably going offline, it should automatically roll back to the last known optimal runtime and notify the maintenance and development teams.

On the administrative level, because inside jobs factor into one of the top entry points of attack, we set forth a few rules to lower risks induced by humans. Every individual has a different clearance level, and when accessing sensitive data, they need to verify their identity and be approved for each access. Authorization level is subject to periodic review and re-verification. No single person should be able to view data alone, so paired team access is required; otherwise will be automatically deemed suspicious activity. No amount of effort will assume 100% safety. Thus, in the event of a breach or a potential attack detected, we need our partners to inform all parties involved and prepare for any necessary remediation to affected individuals and organizations. Lastly, as the risk of data leak increases as more subordinate parties are concerned, we aim to

keep our solutions proprietary and the number of service providers to a minimum. When a sub-agreement is required by any third party providing services to us, a board meeting with the security and development teams should be called before they take such an action.

As we carefully evaluate and update security measures, it is expected that some of these measures will fail to be implemented or adhered to for various reasons, be it our partners decided not to follow alone or abruptive employee behaviors, we aim to provide a solution that would work the best when all requirements are met. Furthermore, a strict requirement may become an obstacle for some potential partners for the development and deployment being overwhelmingly laborious, or posing some technical or financial difficulty; thus subsequently limiting joint collaboration. Lastly, the marketing team may reject some of outlined requirements, too, if they fail to reciprocate the necessity of these measures should they become a financial burden.

Because the data passes through multiple layers owned by separate parties, the idea of data ownership becomes unclear. This could arise a number of issues, for example, upon the request of data deletion from the patient, do we have the right to do so, or do we need to wait for a green light from the EHR system, and vice versa. Although we support multiple major data standards and data format standards, new standards being released, or simply a new overhaul to the existing standard could introduce some troubles, namely is it necessary to add corresponding supports. Furthermore, for existing devices and EHR systems that we already support, it may still happen that certain data transmitted may not have a corresponding field in the target system. These are all potential problems we may face not only during the development phase but also after the deployment.

Existing Solutions

Keeping all of the stakeholder and industry requirements in mind, we explored several options available in the market that are aligned with our project and proposed solution. The two kinds of technical solutions on-market include, standalone and interoperable services. Standalone Remote Patient Monitoring services use proprietary management software that links to wireless enabled medical devices. These devices upload their data to the software either periodically or in real-time. Providers have the ability to access the software and easily manage their patients' needs. Companies using standalone services also provide EHR integration for ease of use. The first standalone RPM solution that we looked into was CareSimple™.

CareSimple™ is an end-to-end virtual care solution that integrates into Electronic Health Records (EHRs) to provide hospitals and physician groups with software, medical devices, logistics and professional services required to support their population health services such as Remote Patient Monitoring (RPM), Chronic Care Management (CCM), Transitional Care

Management (TCM), and Principal Care Management (PCM). Featuring a wide range of cellular and Bluetooth medical devices, an optional senior-friendly mobile application for patients, an easy-to-integrate clinical portal for care managers, flexible care plans, secured messaging, in-app video calling, automated alerts, advanced data analytics and validated educational content, CareSimple™ is delivered directly to patients and requires minimal training and changes in workflow for healthcare professionals. Powered by digital health pioneer Tactio Health, CareSimple™ is the simple, secure, and scalable way to offer remote patient monitoring to large patient populations.

Research into other RPM vendors like HealthSnap and Optimize Health demonstrates that all vendors offer similar devices with comparable capabilities. They differentiate themselves based on the management and analysis software and the level of interoperability they provide.(see Figure 3 CareSimple™ devices offered).

Figure 3: CareSimple™ RPM devices

Next, we focused on the interoperability aspect of Remote Patient Monitoring devices. Both CareSimple™ and HealthSnap use RedoxEngine for EHR integration. Redox, through its FHIR APIs, standardizes integration across a range of devices and softwares including EHR systems. The largest benefit of having a RedoxEngine integration is that it reduces burden on technology teams. With deep integration, providers do not have to learn a multitude of workflows. Some RPM systems are viewable from within the EHR itself, thus saving provider time and displaying required information where appropriate (see Figure 4 sample Redox workflow below).

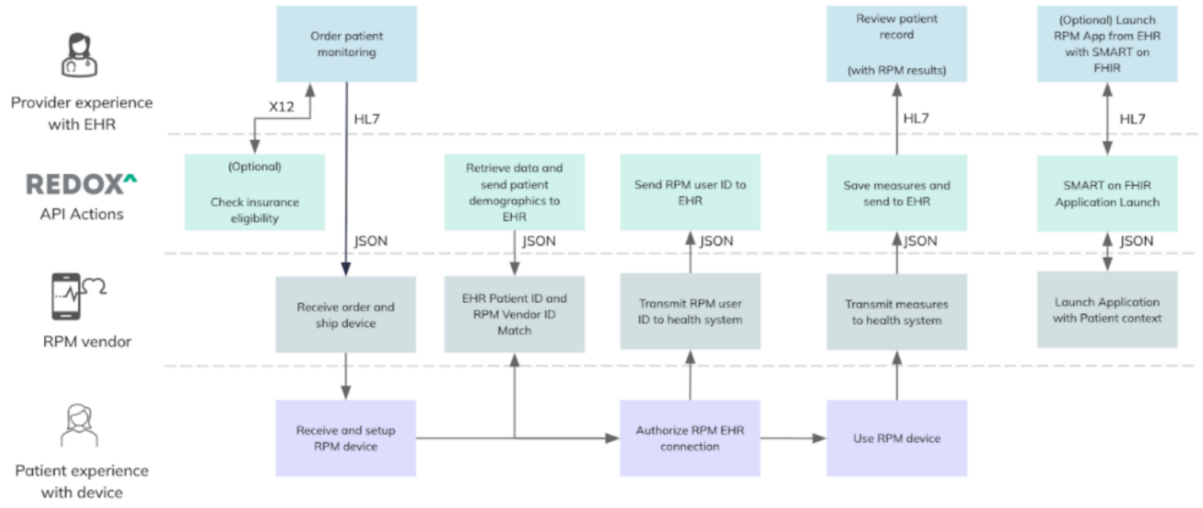


Figure 4: Sample Redox workflow

As demonstrated in Figure 4, Redox provides a layer between the RPM vendor and the EHR. This layer has important security implications which protects and preserves the integrity of PHI and the EHR. Redox also meets all of the security requirements. It ensures that its systems and environments are compliant with relevant standards, including HIPAA, HITRUST and SOC2. Redox is also aligned with the NIST Cybersecurity Framework.Their security team requires an annual audit of all third parties. Any encrypted data is exchanged over either TLS(APIs) or VPN. Redox is hosted in AWS in the US-EAST-1 and CA-CENTRAL-1 regions, with appropriate replication strategies for redundancy and disaster recovery. It uses AWS encryption to encrypt all databases, data stores and file systems.Since any communication between the RPM vendor and the EHR is done through FHIR APIs, there is no threat to the EHR even if the RPM vendor's security is compromised.

In addition, Redox is capable of direct medical device linkage. Partnered with companies like Abbot, Redox enables their devices to work on the Redox network. This workflow opens up another avenue for us - using excellent Redox APIs, we can develop our own interfaces on top and link them to EHR or other data sources. The compose feature from Redox allows us to utilize multiple data sources ,including the EHR, to build standalone software. This makes software development easier and allows broad spectrum analysis to be conducted (see Figure 5 below).

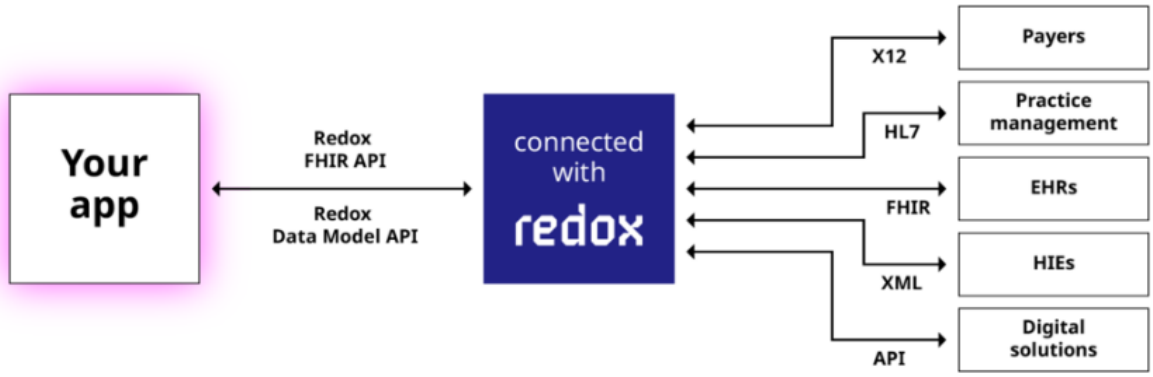


Figure 5: Redox API connection system workflow

Redox is a fantastic service which addresses the security, interoperability and communication needs between multiple systems working with PHI. Any RPM service that we select will be on the Redox network as it meets all stakeholder concerns and the requirements addressed above. Currently, the RPM market is dominated by a limited range of devices and use cases. As the number and types of devices increase, interoperability becomes a larger and more complex challenge. Multiple vendors accessing the EHR increases security risk, complicates integration, and forces providers and technical staff to learn new workflows. Based on the current market, Redox is projected to become an industry standard for interoperability and ensures integration is simple and effective. However, we should strive for a diversified portfolio to mitigate concentration risk and avoid over-reliance on one single asset or strategy which can create a single point of failure and have potentially disastrous results.

Conclusion

Based on our research and industry goals, we recommend using a RPM vendor which is on the Redox Network ensuring high levels of security, efficient and in depth EHR integration. As discussed above, it is important to consider challenges and security when dealing with sensitive health information, however, the benefits of integrating such technology within the healthcare system may offer positive outcomes for all stakeholders involved while aligned with industry objectives such as Meaningful Use. Considering the RPM vendor, doctors and health care providers should make their selection based on current/specific clinical workflows, patient population, and devices offered.

References

Anumula, N, and P C Sanelli. “Meaningful Use.” AJNR. American Journal of Neuroradiology, U.S. National Library of Medicine, Sept. 2012, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7966550/.

Charles, Megan, and Alex DelVecchio. “What Is Meaningful Use?: Definition from TechTarget.” Health IT, TechTarget, 31 Dec. 2018, https://www.techtarget.com/searchhealthit/definition/meaningful-use#:~:text=In%20the%20context%20of%20health,and%20between%20providers%20and%20patients.

Dwivedi, Ruby et al. “Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review.” Journal of oral biology and craniofacial research vol. 12,2 (2022): 302-318. doi:10.1016/j.jobcr.2021.11.010

“IOT in Healthcare: Benefits, Challenges and Applications.” Valuecoders, https://www.valuecoders.com/blog/technology-and-apps/iot-in-healthcare-benefits-challenges-and-applications/.

Kumar, Ashok. “Wearables Device Data Security & Protection.” Voler Systems, Voler Systems, 5 June 2021, https://www.volersystems.com/blog/wearable-devices-data-security.

Luthria, Gaurav, and Qingbo Wang. “Implementing a Cloud Based Method for Protected Clinical Trial Data Sharing.” Pacific Symposium on Biocomputing. Pacific Symposium on Biocomputing vol. 25 (2020): 647-658.

“Managing Chronic Conditions through Telehealth.” Telehealth.hhs.gov, Health Resources and Services Administration, https://telehealth.hhs.gov/providers/best-practice-guides/telehealth-for-chronic-conditions/managing-chronic-conditions-through-telehealth.

Madjid Karimi. “National Survey Trends in Telehealth Use in 2021: Disparities in Utilization and Audio vs. Video Services.” ASPE, https://www.aspe.hhs.gov/reports/hps-analysis-telehealth-use-2021.

Mehrtak, Mohammad et al. “Security challenges and solutions using healthcare cloud computing.” Journal of medicine and life vol. 14,4 (2021): 448-461. doi:10.25122/jml-2021-0100

Olmedo-Aguirre, José Oscar et al. “Remote Healthcare for Elderly People Using Wearables: A Review.” Biosensors vol. 12,2 73. 27 Jan. 2022, doi:10.3390/bios12020073

“Remote Patient Monitoring Statistics 2023: Trends and the Future Perspectives.” Gitnux, 24 Mar. 2023, https://blog.gitnux.com/remote-patient-monitoring-statistics/.

Syagnik (Sy) Banerjee, Thomas Hemphill & Phil Longstreet (2018) Wearable devices and healthcare: Data sharing and privacy, The Information Society, 34:1, 49-57, DOI: 10.1080/01972243.2017.1391912